+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 19/03/2026

S'inscrire

Formation Certification SailPoint Identity Security Expert

3 jours (21 heures)

Présentation

La certification SailPoint Identity Security Expert Credential valide votre capacité à concevoir, configurer et opérer une solution IGA orientée sécurité des identités. Vous apprendrez à répondre à des cas d'usage concrets : joiner/mover/leaver, demandes d'accès, recertifications et réduction du risque.

Cette formation vous prépare à l'examen en couvrant les concepts clés (gouvernance, rôles, politiques, connecteurs) et leur mise en œuvre dans SailPoint. L'objectif est de transformer les exigences métiers et conformité en contrôles techniques mesurables.

L'approche est résolument pratique : démos guidées, ateliers de configuration, analyse d'erreurs fréquentes et scénarios d'exploitation. Vous repartez avec des checklists de préparation, des modèles de paramétrage et une méthodologie pour diagnostiquer les problèmes d'intégration et de gouvernance.

Objectifs

- Configurer les composants essentiels d'une plateforme SailPoint orientée IGA.
- Mettre en place des workflows de demandes d'accès et d'approbations.
- Définir rôles, politiques et règles de conformité (SoD, exceptions).
- Orchestrer le cycle de vie des identités (JML) et les provisioning.
- Analyser logs, campagnes et rapports pour réduire le risque et améliorer l'auditabilité.

Public visé

- Ingénieurs IAM / IGA
- Administrateurs SailPoint
- Consultants sécurité et gouvernance
- Architectes identité

Pré-requis

- Notions solides d’IAM (authentification, autorisation, RBAC/ABAC).
- Compréhension des annuaires et référentiels (AD, LDAP, RH).
- Connaissances de base en SQL et lecture de logs.
- Notions de conformité/audit (recertification, SoD).

Pré-requis techniques

- PC avec 8 Go RAM minimum (16 Go recommandé) et CPU récent.
- Windows 10/11, macOS ou Linux avec navigateur moderne.
- Accès à un environnement SailPoint de formation et connectivité réseau stable.
- Éditeur de texte, terminal

Programme de notre formation Certification SailPoint Identity Security Expert Credential

[Jour 1 - Matin]

Fondamentaux IAM et périmètre SailPoint Identity Security

- Rappels IAM/IGA : identité, comptes, droits, rôles, séparation des tâches
- Positionnement SailPoint : Identity Security Cloud, cas d’usage et bénéfices
- Concepts clés : sources, entitlements, access profiles, roles
- Lecture des exigences de la certification : domaines, types de questions, stratégie d’étude
- Atelier pratique : Cartographier un SI cible (sources, applications, droits) et le modèle IGA associé

[Jour 1 - Après-midi]

Onboarding des sources et modélisation des accès

- Onboarding d’une source : connectivité, schémas d’attributs, corrélation d’identités
- Modéliser les droits : entitlements et regroupements en access profiles
- Bonnes pratiques de nommage, descriptions, owners et gouvernance des objets
- Contrôles de qualité : doublons, droits orphelins, attributs manquants, cohérence des données
- Atelier pratique : Créer une source de démonstration et construire 2 access profiles alignés sur un besoin métier

[Jour 2 - Matin]

Gestion du cycle de vie (Joiner/Mover/Leaver) et provisioning

- Événements JML : déclencheurs, attributs RH, règles d’affectation et exceptions
- Provisioning : demandes, approbations, exécution, suivi des erreurs et relances
- Gestion des comptes : création, mise à jour, désactivation, suppression, réconciliation
- Traçabilité : journaux, états, preuves et bonnes pratiques d’audit
- Atelier pratique : Configurer un scénario JML (arrivée + départ) et valider les actions attendues

[Jour 2 - Après-midi]

Workflows, politiques et gouvernance des demandes d’accès

- Chaînes d’approbation : managers, owners, approbations conditionnelles et escalades
- Politiques : contrôles de conformité, règles de SoD, détection de conflits
- Gestion des exceptions : compensations, justifications, durées et revues périodiques
- Expérience utilisateur : catalogue, recherche, recommandations et rationalisation des demandes
- Atelier pratique : Concevoir un workflow de demande avec SoD et une exception contrôlée

[Jour 3 - Matin]

Rôles, access modeling avancé et bonnes pratiques d’architecture

- Stratégies de role mining et approche itérative (MVP, durcissement, adoption)
- Conception de rôles : métiers vs techniques, hiérarchies, héritage et maintenance
- Alignement rôles / access profiles : granularité, réutilisabilité et gouvernance
- Architecture : environnements, séparation des responsabilités, gestion des changements
- Atelier pratique : Définir un modèle de rôles (3 rôles) et le relier à des access profiles existants

[Jour 3 - Après-midi]

Certification readiness : access reviews, reporting et préparation à l’examen

- Campagnes d’access reviews : périmètre, échantillonnage, délégations, décisions et preuves
- Reporting & audit : indicateurs, exports, contrôles clés et points de vigilance
- Résolution de cas : erreurs de corrélation, droits persistants, écarts entre source et IGA
- Révision ciblée : questions types, pièges fréquents, gestion du temps et check-list finale
- Atelier pratique : Exécuter une mini-campagne de revue d’accès et produire les éléments de preuve attendus

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.